日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年１０月　５日

出願番号
Application Number: 特願２００１－３０９６７０

出願人
Applicant(s): 日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年１０月２６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０９３６２６

【書類名】　特許願

【整理番号】　413001045

【提出日】　平成13年10月 5日

【あて先】　特許庁長官殿

【国際特許分類】　H04N 7/167

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　髙口　達至

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　臼田　典弘

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　泊野　和広

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　寺田　雅彦

【電話番号】　045-450-2423

【先の出願に基づく優先権主張】

【出願番号】　特願2001- 87799

【出願日】　平成13年 3月26日

【手数料の表示】

【予納台帳番号】　003654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　画像表示装置

【特許請求の範囲】

【請求項１】

暗号化された映像信号を認証して復号する認証・復号部と、映像信号を画像表示する表示部とを備えた画像表示装置において、

前記画像表示装置の筐体の開放を検出する開放検出手段と、

前記認証・復号部における認証動作を有効とすることを示す第１のフラグと、前記認証・復号部における認証動作を無効とすることを示す第２のフラグとのいずれかのフラグを記憶する記憶手段と、

前記開放検出手段によって前記筐体の開放が検出されたら、前記記憶手段に前記第２のフラグを書き込むよう制御するフラグ書き込み手段と、

前記記憶手段に記憶されたフラグに応じて、前記認証・復号部における認証動作を有効とするか無効とするかを制御する有効・無効制御手段と、

前記記憶手段に記憶されたフラグが前記第１のフラグであるとき、前記暗号化された映像信号を復号した映像信号を前記表示部に画像表示することにより、前記表示部を第１の状態とする第１の表示部制御手段と、

前記記憶手段に記憶されたフラグが前記第２のフラグであるとき、前記表示部を前記第１の状態とは異なる第２の状態とする第２の表示部制御手段とを備えて構成したことを特徴とする画像表示装置。

【請求項２】

前記フラグ書き込み手段によって、前記第２のフラグが記憶された前記記憶手段に前記第１のフラグを書き込ませることにより、前記認証・復号部における認証動作を有効な状態に戻すための隠しコマンドを入力する入力手段を備えて構成したことを特徴とする請求項１記載の画像表示装置。

【請求項３】

前記画像表示装置の電源が切断されたときでも前記開放検出手段と前記記憶手段と前記フラグ書き込み手段が動作するよう、前記開放検出手段と前記記憶手段と前記フラグ書き込み手段に電源を供給する独立電源を備えて構成したことを特

徴とする請求項１または２に記載の画像表示装置。

【請求項４】

暗号化された映像信号を認証して復号する認証・復号部と、映像信号を画像表示する表示部とを備えた画像表示装置において、

前記認証・復号部によって前記暗号化された映像信号を復号した映像信号が前記画像表示装置外へと取り出されるおそれが発生したことを検出する検出手段と、

前記認証・復号部における認証動作を有効とすることを示す第１のフラグと、前記認証・復号部における認証動作を無効とすることを示す第２のフラグとのいずれかのフラグを記憶する記憶手段と、

前記検出手段によって前記暗号化された映像信号を復号した映像信号が前記画像表示装置外へと取り出されるおそれが発生したことが検出されたら、前記記憶手段に前記第２のフラグを書き込むよう制御するフラグ書き込み手段と、

前記記憶手段に記憶されたフラグに応じて、前記認証・復号部における認証動作を有効とするか無効とするかを制御する有効・無効制御手段と、

前記記憶手段に記憶されたフラグが前記第１のフラグであるとき、前記暗号化された映像信号を復号した映像信号を前記表示部に画像表示することにより、前記表示部を第１の状態とする第１の表示部制御手段と、

前記記憶手段に記憶されたフラグが前記第２のフラグであるとき、前記表示部を前記第１の状態とは異なる第２の状態とする第２の表示部制御手段とを備えて構成したことを特徴とする画像表示装置。

【請求項５】

前記フラグ書き込み手段によって、前記第２のフラグが記憶された前記記憶手段に前記第１のフラグを書き込ませることにより、前記認証・復号部における認証動作を有効な状態に戻すための隠しコマンドを入力する入力手段を備えて構成したことを特徴とする請求項４記載の画像表示装置。

【請求項６】

前記画像表示装置の電源が切断されたときでも前記検出手段と前記記憶手段と前記フラグ書き込み手段が動作するよう、前記検出手段と前記記憶手段と前記フ

ラグ書き込み手段に電源を供給する独立電源を備えて構成したことを特徴とする請求項４または５に記載の画像表示装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化された映像信号を復号処理して画像表示する画像表示装置に係り、特に、暗号を解いた映像信号を不正に取得したり、不正に複製することを防止することができる画像表示装置に関する。

【０００２】

【従来の技術】

画像表示装置のような映像信号を扱う映像機器において、映像信号（コンテンツ）の著作権保護は重要な問題である。近年のデジタル技術は放送・映像分野にも広がっており、家庭用テレビジョン受像機等の画像表示装置においても、デジタル映像信号を扱うようになってきている。デジタル映像信号の一例として、不正に複製することができないように暗号化されたベースバンドのデジタル映像信号がある。この種のデジタル映像信号を扱う画像表示装置は、暗号を解くための復号部を備え、復号部によって暗号を解いて映像信号を表示部に画像表示する。

【０００３】

【発明が解決しようとする課題】

ところで、画像表示装置の内部では、コネクタやワイヤあるいは回路基板上の配線が至る所で露出している。復号部より出力される映像信号は暗号が解かれているので、悪意を有するものが、画像表示装置の筐体（カバー）を開け、復号部より出力された暗号が解かれた状態の映像信号を不正に外部へと取り出すことが可能である。よって、何らかの処置を講じない限り、映像信号（コンテンツ）の不正な取得や複製を防ぐことができないという問題点がある。

【０００４】

この不正な取得や複製を防ぐ１つの手段として、画像表示装置の内部におけるコネクタ，ワイヤ，配線等の露出部分に保護を施し、露出部分をなくすことにより映像信号の外部への取り出しを防ぐというものがある。しかしながら、これで

は、画像表示装置としての設計の自由度を低下させ、また、コストを上昇させることになるので好ましい方法ではない。さらに、露出部分の保護を取り外して、映像信号を取り出すことも比較的容易であり、不正な取得や複製を効果的に防ぐ方法であるとは言いがたい。

【０００５】

今後、暗号化された映像信号は増えるものと予想され、不正な取得や複製を防いで、コンテンツの著作権を保護する必要性はますます高まると思われる。よって、暗号化された映像信号の著作権をどのようにして保護するかは、極めて重要な問題であり、効果的な解決策が望まれていた。

【０００６】

本発明はこのような問題点に鑑みなされたものであり、暗号化された映像信号の不正な取得や複製を、比較的簡単な方法でかつ効果的に防ぐことができる画像表示装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】

本発明は、上述した従来の技術の課題を解決するため、

（ａ）暗号化された映像信号を認証して復号する認証・復号部（２）と、映像信号を画像表示する表示部（５）とを備えた画像表示装置において、前記画像表示装置の筐体（１０）の開放を検出する開放検出手段（８）と、前記認証・復号部における認証動作を有効とすることを示す第１のフラグと、前記認証・復号部における認証動作を無効とすることを示す第２のフラグとのいずれかのフラグを記憶する記憶手段（７）と、前記開放検出手段によって前記筐体の開放が検出されたら、前記記憶手段に前記第２のフラグを書き込むよう制御するフラグ書き込み手段（６）と、前記記憶手段に記憶されたフラグに応じて、前記認証・復号部における認証動作を有効とするか無効とするかを制御する有効・無効制御手段（６）と、前記記憶手段に記憶されたフラグが前記第１のフラグであるとき、前記暗号化された映像信号を復号した映像信号を前記表示部に画像表示することにより、前記表示部を第１の状態とする第１の表示部制御手段（２，４）と、前記記憶手段に記憶されたフラグが前記第２のフラグであるとき、前記表示部を前記第１

の状態とは異なる第２の状態とする第２の表示部制御手段（２，４）とを備えて構成したことを特徴とする画像表示装置（１００）を提供し、

（ｂ）暗号化された映像信号を認証して復号する認証・復号部（２）と、映像信号を画像表示する表示部（５）とを備えた画像表示装置において、前記認証・復号部によって前記暗号化された映像信号を復号した映像信号が前記画像表示装置外へと取り出されるおそれが発生したことを検出する検出手段（８）と、前記認証・復号部における認証動作を有効とすることを示す第１のフラグと、前記認証・復号部における認証動作を無効とすることを示す第２のフラグとのいずれかのフラグを記憶する記憶手段（７）と、前記検出手段によって前記暗号化された映像信号を復号した映像信号が前記画像表示装置外へと取り出されるおそれが発生したことが検出されたら、前記記憶手段に前記第２のフラグを書き込むよう制御するフラグ書き込み手段（６）と、前記記憶手段に記憶されたフラグに応じて、前記認証・復号部における認証動作を有効とするか無効とするかを制御する有効・無効制御手段（６）と、前記記憶手段に記憶されたフラグが前記第１のフラグであるとき、前記暗号化された映像信号を復号した映像信号を前記表示部に画像表示することにより、前記表示部を第１の状態とする第１の表示部制御手段（２，４）と、前記記憶手段に記憶されたフラグが前記第２のフラグであるとき、前記表示部を前記第１の状態とは異なる第２の状態とする第２の表示部制御手段（２，４）とを備えて構成したことを特徴とする画像表示装置（１００）を提供するものである。

【０００８】

【発明の実施の形態】

以下、本発明の画像表示装置について、添付図面を参照して説明する。図１は本発明の画像表示装置の一実施形態を示すブロック図、図２は本発明の画像表示装置の動作を説明するためのフローチャート、図３は本発明の画像表示装置の他の実施形態を示すブロック図である。

【０００９】

図１において、本発明の一実施形態である画像表示装置１００と、セットトップボックスまたはＤ－ＶＨＳ（本出願人の登録商標）等の映像信号出力装置２０

０とが、ケーブル３００にて接続されている。ケーブル３００のコネクタ３０１が映像信号出力装置２００の出力端子２０１に接続され、コネクタ３０２が画像表示装置１００の入力端子１に接続されている。映像信号出力装置２００によって再生あるいは復調して得た、暗号化されたベースバンドのデジタル映像信号（以下、暗号化映像信号）は、ケーブル３００によって伝送され、画像表示装置１００に入力される。なお、暗号化されたデジタル映像信号はベースバンドに限定されるものではなく、圧縮された信号であってもよい。

【００１０】

本実施形態では、暗号化映像信号はＲ，Ｇ，Ｂの３原色信号であり、画像表示装置１００と映像信号出力装置２００との間では、ケーブル３００によって、Ｒ，Ｇ，Ｂ信号の他、各種の制御信号の伝送（通信）も行われる。入力端子１より入力されたＲ，Ｇ，Ｂ信号は、認証・復号部２に入力される。認証・復号部２は、鍵データ保持部３に保持された鍵データを用いて、ケーブル３００を介して、映像信号出力装置２００と認証手続きのための通信を行う。この認証のための通信の結果、認証が得られるか否か（暗号を解いてよいか否か）を判断し、認証が得られたときのみ、暗号を解いたＲ，Ｇ，Ｂ信号を出力する。

【００１１】

マイクロコントローラ６は、認証・復号部２によって実際に認証動作を行わせるか否かを制御する。これについては後に詳述する。鍵データ保持部３は、例えば、リード・オンリ・メモリ（ＲＯＭ）よりなる。認証・復号部２が鍵データ保持部３より入力された鍵データをどのように処理するか、映像信号出力装置２００と認証・復号部２とが認証のためにどのような内容をやり取りするかについては、暗号化映像信号の著作権保護のため、明らかにされるものではない。

【００１２】

認証・復号部２より出力されたＲ，Ｇ，Ｂ信号は、映像処理部４に入力される。映像処理部４は画質調整等の通常の映像処理を施し、陰極線管（ＣＲＴ）等の表示部５に供給する。これにより、表示部５には、暗号化映像信号を復号した映像信号が画像表示される。表示部５は、ＣＲＴに限定されるものではなく、映像を投射するためのスクリーン、プラズマディスプレイ等の任意の表示手段である

。なお、暗号化映像信号ではなく、図示していない他の入力端子や内蔵のチューナ等より得た暗号化されていない通常の映像信号は、認証・復号部２を介することなく、映像処理部４に入力されて表示部５に画像表示されることになる。

【００１３】

次に、暗号化映像信号を復号した映像信号の不正な取得や複製を防ぐ具体的構成について説明する。マイクロコントローラ６には、メモリ７と、筐体１０の開放を検出する開放検出器８と、操作部９が接続されている。開放検出器８は一例として硫化カドミウムセル（ＣｄＳセル）やシリコンダイオード等の光センサよりなり、周囲の明るさを検知することにより筐体１０が開放されたか否かを検出する。開放検出器８を光センサによって構成した場合、筐体１０を閉じた状態（フロントカバーにリアカバーを装着した状態）と、筐体１０を開放した状態（リアカバーをフロントカバーより取り外した状態）との照度の差を検出するよう光センサの周辺回路を構成する。この場合、光センサの光感知部を、例えば、リアカバーに密着させる等が考えられる。

【００１４】

メモリ７には、工場出荷時の初期状態として、認証・復号部２による認証動作を有効とする（認証動作を許可する）ことを示すフラグ（例えば、“０”）が書き込まれている。暗号化映像信号を復号した映像信号の外部への取り出しを試みようとする者が、筐体１０を開けると、開放検出器８がそれを検出し、マイクロコントローラ６に検出信号を供給する。マイクロコントローラ６は、開放検出器８から検出信号が入力されると、認証・復号部２による認証動作を無効とする（認証動作を許可しない）フラグ（例えば、“１”）をメモリ７に上書きにより書き込む。マイクロコントローラ６は、フラグ書き込み手段として動作している。

【００１５】

マイクロコントローラ６は、メモリ７に書き込まれているフラグが、認証・復号部２による認証動作を無効とするフラグ（“１”）であれば、認証・復号部２によって認証動作を行わせないよう認証・復号部２を制御する。マイクロコントローラ６は、認証・復号部２における認証動作を有効とするか無効とするかを制御する有効・無効制御手段としても動作している。

【００１６】

よって、一旦、筐体１０を開けると、暗号化映像信号は認証・復号部２による認証動作が行われないので、たとえ、本来であれば認証動作を行って暗号を解いてよいと判断される正規の暗号化映像信号であったとしても、認証・復号部２からは、暗号化映像信号がそのまま出力される。よって、映像信号の不正な取得や複製を試みようとする者が、暗号化映像信号を復号した映像信号を筐体１０の外部へと取り出すことはできない。このとき、表示部５には、暗号化映像信号がそのまま表示されることになるので、ノイズが表示された状態となる。

【００１７】

メモリ７は不揮発性メモリであるので、画像表示装置１００の電源を一旦切断しても、メモリ７のフラグが消えてしまうことはない。よって、筐体１０を閉めて再び電源を投入しても、後述する復元操作を行わない限り、認証・復号部２による認証動作を有効な状態に戻すことはできない。なお、マイクロコントローラ６とメモリ７と開放検出器８の電源を、画像表示装置１００の電源（図示せず）とは連動しない独立の電源（バックアップ電源）とすれば、画像表示装置１００の電源を投入していない状態での筐体１０の開放も検出することができる。画像表示装置１００の電源を投入していない状態でも筐体１０の開放を検出するよう構成することは、より好ましい実施形態である。

【００１８】

図３に、画像表示装置１００の電源を投入していない状態でも筐体１０の開放を検出するよう構成したより好ましい実施形態を示す。図３において、図１と同一部分には同一符号を付し、その説明を適宜省略する。図３に示すように、画像表示装置１００には、画像表示装置１００の電源（主電源）とは別の独立電源１１が設けられている。独立電源１１は、電池や大容量コンデンサ等を用いて構成する。画像表示装置１００の電源が切断されても、独立電源１１によってマイクロコントローラ６とメモリ７と開放検出器８に電源が供給されて、これらが動作するようになっている。なお、画像表示装置１００の電源が切断されたときのみ、電源１１が使用されるよう構成することが望ましい。

【００１９】

この構成により、画像表示装置１００の電源を投入していない状態での筐体１０の開放も検出することができ、暗号化された映像信号の不正な取得や複製を、さらに効果的に防ぐことが可能となる。

【００２０】

なお、以上の例では、開放検出器８が筐体１０の開放を検出すると説明したが、筐体１０に穴を開けるとか、筐体１０を破壊する等でも同様に検出することが可能である。筐体１０の開放とは、カバーを開けること、穴を開けること、破壊すること等の全てを含み、これらと実質的に同一のものは全て“開放”に含まれる。開放検出器８としては、光センサに限定されず、機械的なスイッチ等の機械的センサであってもよい。また、光センサと機械的センサとを組み合わせてもよく、開放検出器８の構成は任意でよい。

【００２１】

マイクロコントローラ６としては、ごく小規模のプログラムを低速で動作させるだけの能力があれば十分である。マイクロコントローラ６は、認証・復号部２における認証動作の有効・無効を制御するための専用のものであってもよく、他の機能を行うためのものと兼用させてもよい。また、マイクロコントローラ６として、プログラムメモリや不揮発性メモリを内蔵し、プログラムメモリにプログラムを書き込んだ後にその読み出しに対してプロテクトをかけることができるものを用いれば、プログラムの読み出しも防ぐことが可能である。この種のマイクロコントローラでも安価であり、画像表示装置１００がさほど高価になることはない。

【００２２】

以上のようにして、本発明の画像表示装置１００では、暗号化映像信号を復号した映像信号の不正な取得や複製が行われるおそれのある、筐体１０が開放されたときには、マイクロコントローラ６の制御によって認証・復号部２による認証動作が無効（不許可）とされるので、暗号化映像信号を復号した映像信号を、外部へと取り出すことはできず、コンテンツの著作権が保護される。なお、本発明の画像表示装置１００では、認証・復号部２において認証動作が有効とされる場合においても、鍵の不一致等の暗号を解くべきではない状態が発生したときには

、当然のことながら、暗号化映像信号の暗号を解く認証は得られない。

【００２３】

画像表示装置１００の工場における生産時や修理や点検を行ういわゆるサービス時にも、筐体１０を開放する場合がある。このような場合でも、上記の認証動作無効の制御が行われてしまうことになる。そこで、一旦、認証・復号部２による認証動作が無効とされたものを元の有効な状態に戻して復元（再起動）させるよう構成することが必要となる。

【００２４】

図１，図３において、操作部９は、認証・復号部２による認証動作が無効とされたものを有効な状態に戻す復元操作を行うために設けている。操作部９は画像表示装置１００に設けたスイッチ（操作釦）であってもよく、図１，図３では筐体１０内に設けているが、筐体１０外のリモコン送信機であってもよい。操作部９としては、復元操作を行うため専用である必要はなく、電源スイッチ等の他の操作スイッチと兼用であってもよい。操作部９によって復元のためのパスワードを入力したり、予め定められたジャンパやスイッチの設定を行うことによって、マイクロコントローラ６に復元の指示を与えることができる。これらのパスワードやジャンパ，スイッチの設定は、復元のための隠しコマンドである。

【００２５】

マイクロコントローラ６は、操作部９による隠しコマンドの入力によって、認証動作復元の指示が入力されたら、メモリ７を初期化し、認証・復号部２による認証動作を有効とすることを示すフラグ（“０”）に戻す。これにより、認証・復号部２による認証動作は初期状態である有効な状態に戻り、認証・復号部２は再び映像信号出力装置２００との間で認証手続きのための通信を行い、暗号化映像信号を復号することができるようになる。

【００２６】

以上の本発明の画像表示装置１００の動作を、図２のフローチャートを用いて改めて説明する。図２において、ステップＳ１にて、操作部９によって隠しコマンドが入力され、再起動モードとされたか否かを判定する。再起動モードであれば、ステップＳ２にて、メモリ７を初期化する復元処理を行い、ステップＳ３に

移る。再起動モードでなければ、そのままステップＳ３に移る。ステップＳ３では、メモリ７のフラグをチェックし、認証・復号部２による認証動作が有効の状態であるか無効の状態であるかを判定する。認証・復号部２による認証動作が無効の状態であれば、ステップＳ７に移る。

【００２７】

ステップＳ３で認証・復号部２による認証動作が有効の状態であれば、ステップＳ４にて、筐体１０が開放されたか否かを判定する。筐体１０が開放されたと判定されなければ、ステップＳ６に移る。ステップＳ６にて、暗号化映像信号を復号した映像信号の画像表示が行われ、ステップＳ１に戻る。筐体１０が開放されたと判定されれば、ステップＳ５に移り、ステップＳ５にて、メモリ７に、認証・復号部２による認証動作を無効とするフラグ（“１”）を上書きする。そして、ステップＳ７に移る。ステップＳ７では、暗号化映像信号を復号した映像信号の画像表示を非表示とする処理が行われ、ステップＳ１に戻る。

【００２８】

以上のステップＳ１～Ｓ７は、常時または所定の時間間隔で繰り返される。なお、ステップＳ１～Ｓ５は、マイクロコントローラ６における処理や判断である。ステップＳ６及びＳ７は、認証・復号部２，映像処理部４，表示部５における処理である。ステップＳ７における、暗号化映像信号を復号した映像信号の画像表示を非表示とする処理とは、本実施形態では、認証・復号部２による認証動作が無効の状態では認証・復号部２による認証動作が行われず、暗号化映像信号を復号した映像信号が出力されないので、暗号化映像信号を復号した映像信号が表示部５に表示されない状態である。

【００２９】

ステップＳ７における画像表示を非表示とする処理には、暗号化映像信号がそのまま認証・復号部２より出力されて、表示部５にノイズが表示された状態となることの他、映像処理部４にて、目障りなノイズをミュートさせて無信号状態としたり、青等の単色を表示することや、暗号化映像信号を認証できなくなった旨や不正のおそれがあるため暗号化映像信号の表示を停止した旨等の警告信号を表示部５にオンスクリーン表示すること等を含む。

【００３０】

ステップＳ６において、暗号化映像信号を復号した映像信号が表示部５に正しく画像表示された状態を第１の状態とすると、認証・復号部２及び映像処理部４は、表示部５を第１の状態とする第１の表示部制御手段となっている。ステップＳ７においては、表示部５にノイズが表示された状態であったり、何も表示しない無信号状態であったり、単色や警告信号が表示された状態であり、表示部５は、第１の状態とは異なる第２の状態となっている。認証・復号部２及び映像処理部４は、表示部５を第２の状態とする第２の表示部制御手段にもなっている。

【００３１】

画像表示装置１００は、当然のことながら、暗号化映像信号を復号した映像信号を外部に出力するための出力端子を備えていない。よって、暗号化映像信号は、画像表示装置１００という閉じた装置内で復号して表示部５に表示させるという目的以外には用いることができない。暗号化映像信号を復号した映像信号が画像表示装置外へと取り出されるおそれが発生しない限りは、第１の表示部制御手段によって、暗号化映像信号を復号した映像信号が表示部５に正しく画像表示される。暗号化された映像信号を復号した映像信号が画像表示装置外へと取り出されるおそれが発生すれば、第２の表示部制御手段によって、暗号化映像信号を復号した映像信号が画像表示されることはない。

【００３２】

なお、暗号化されていない通常の映像信号は、第１，第２の表示部制御手段とは無関係であり、常に表示部５に正しく画像表示される。よって、本発明による暗号化映像信号を復号した映像信号の不正取り出し防止方法は、暗号化されていない通常の映像信号に何らの影響を与えるものではない。

【００３３】

本発明は以上説明した本実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において種々変更可能である。開放検出器８は、認証・復号部２によって暗号化映像信号を復号した映像信号が画像表示装置１００外へと取り出されるおそれが発生したことを比較的簡単に検出する１つの好ましい例であり、より複雑な検出手段を採用してもよい。本実施形態では、暗号化映像信号を外部

の映像信号出力装置２００より供給される信号としたが、これに限定されることはなく、内蔵のチューナやテープカセットまたはディスク等の記録媒体より得た信号であってもよい。

【００３４】

【発明の効果】

以上詳細に説明したように、本発明の画像表示装置は、画像表示装置の筐体の開放を検出する開放検出手段（認証・復号部によって暗号化された映像信号を復号した映像信号が画像表示装置外へと取り出されるおそれが発生したことを検出する検出手段）と、認証・復号部における認証動作を有効とすることを示す第１のフラグと、認証・復号部における認証動作を無効とすることを示す第２のフラグとのいずれかのフラグを記憶する記憶手段と、開放検出手段によって筐体の開放が検出されたら、記憶手段に第２のフラグを書き込むよう制御するフラグ書き込み手段（検出手段によって暗号化された映像信号を復号した映像信号が画像表示装置外へと取り出されるおそれが発生したことが検出されたら、記憶手段に第２のフラグを書き込むよう制御するフラグ書き込み手段）と、記憶手段に記憶されたフラグに応じて、認証・復号部における認証動作を有効とするか無効とするかを制御する有効・無効制御手段と、記憶手段に記憶されたフラグが第１のフラグであるとき、暗号化された映像信号を復号した映像信号を表示部に画像表示することにより、表示部を第１の状態とする第１の表示部制御手段と、記憶手段に記憶されたフラグが前記第２のフラグであるとき、表示部を第１の状態とは異なる第２の状態とする第２の表示部制御手段とを備えて構成したので、暗号化された映像信号の不正な取得や複製を、比較的簡単な方法でかつ効果的に防ぐことができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態を示すブロック図である。

【図２】

本発明の動作を説明するためのフローチャートである。

【図３】

本発明の他の実施形態を示すブロック図である。

【符号の説明】

１　入力端子

２　認証・復号部（第１の表示部制御手段，第２の表示部制御手段）

３　鍵データ保持部

４　映像処理部（第１の表示部制御手段，第２の表示部制御手段）

５　表示部

６　マイクロコントローラ（フラグ書き込み手段，有効・無効制御手段）

７　メモリ（記憶手段）

８　開放検出器（開放検出手段，検出手段）

９　操作部（入力手段）

１０　筐体

１１　独立電源

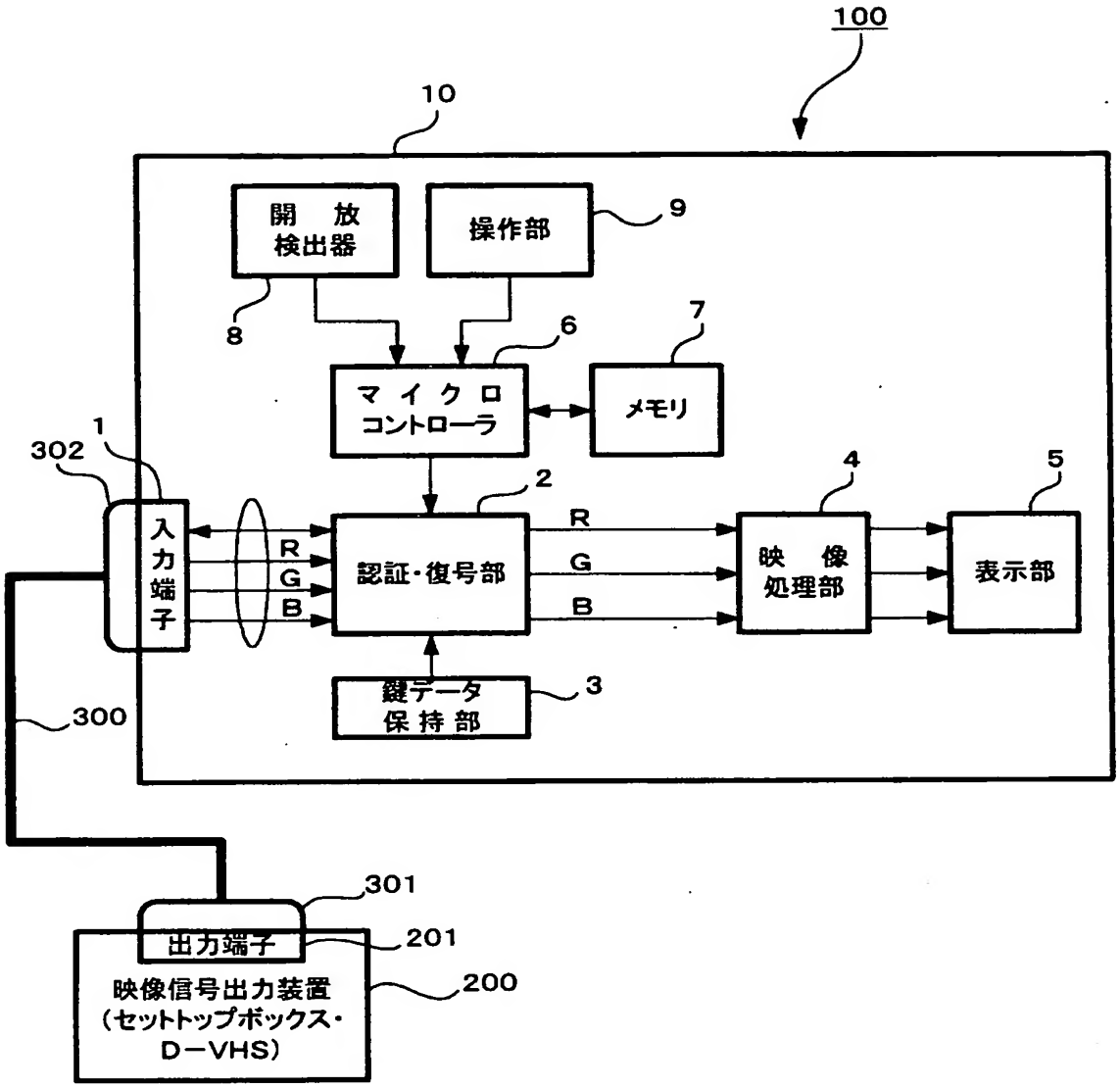
１００　画像表示装置

２００　映像信号出力装置

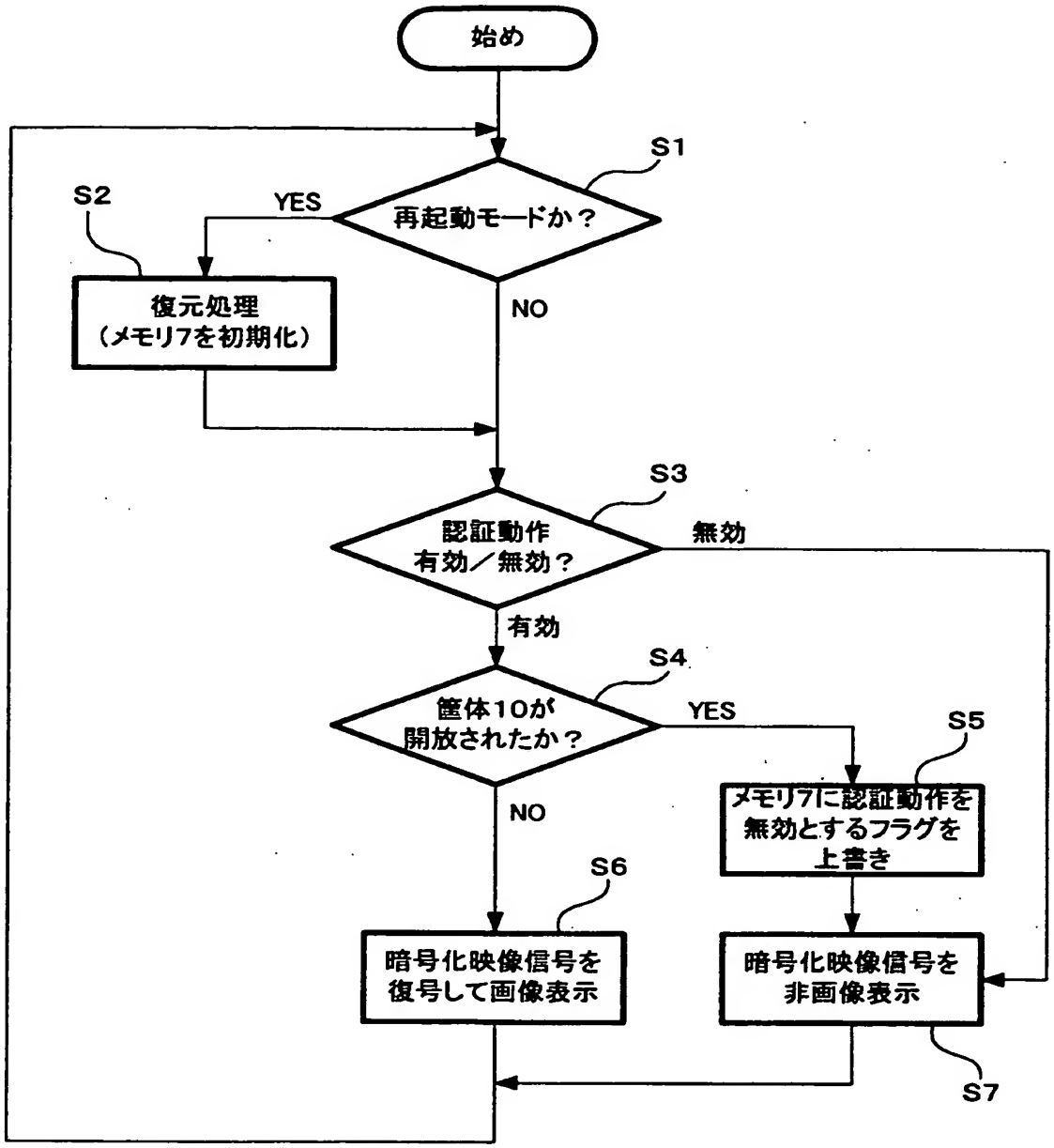
３００　ケーブル

【書類名】　　図面

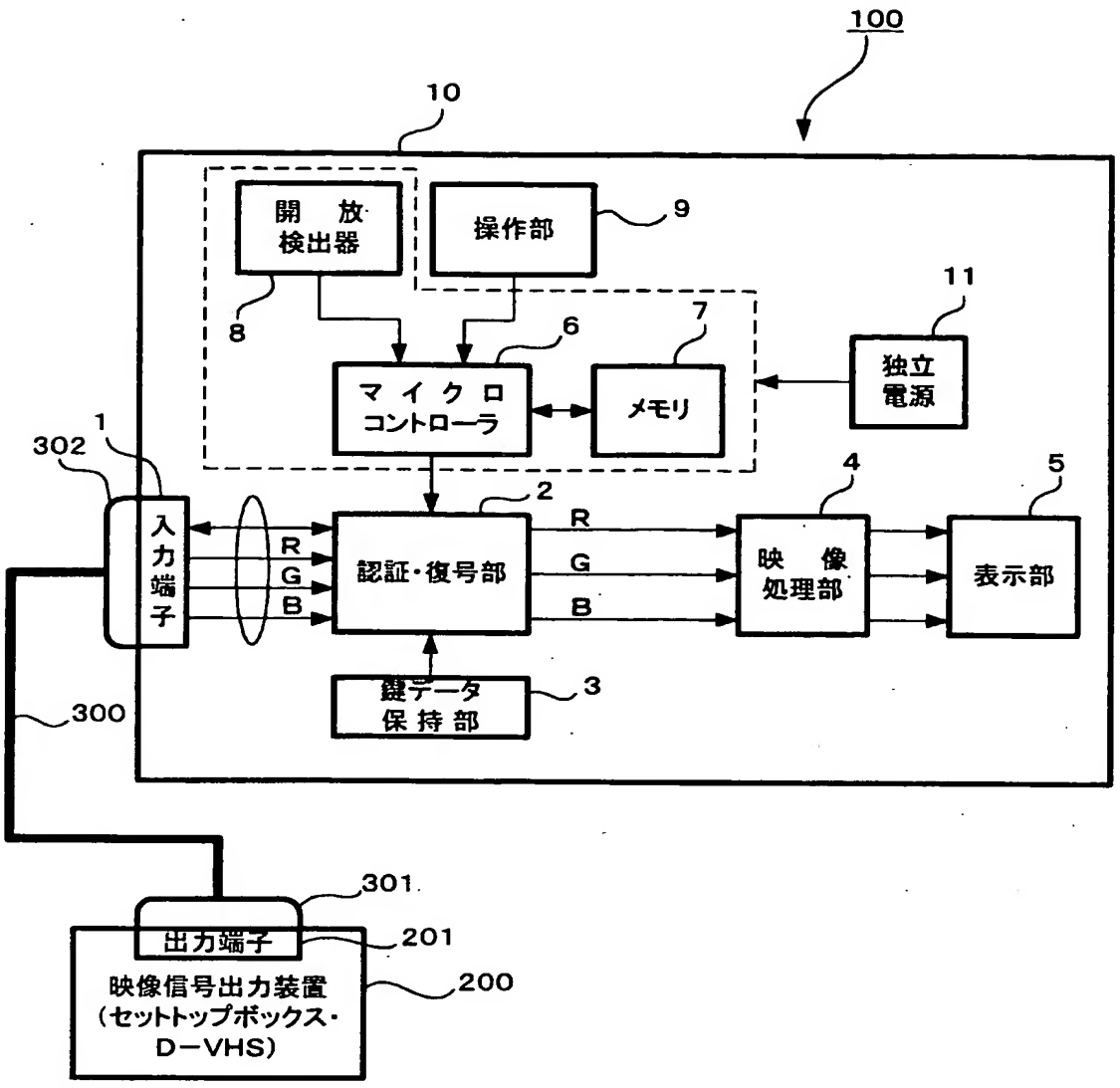
【図１】


100
10
開　放
検出器
操作部
9
8
6
7
マイクロ
コントローラ
メモリ
1
302
2
4
5
入力端子
R
G
B
認証・復号部
R
G
B
映　像
処理部
表示部
鍵データ
保持部
3
300
301
出力端子
201
映像信号出力装置
（セットトップボックス・
D－VHS）
200

【図２】


始め
S1
再起動モードか？
YES
S2
復元処理
（メモリ7を初期化）
NO
S3
認証動作
有効／無効？
無効
有効
S4
筐体10が
開放されたか？
YES
S5
メモリ7に認証動作を
無効とするフラグを
上書き
NO
S6
暗号化映像信号を
復号して画像表示
暗号化映像信号を
非画像表示
S7

【図３】


100
10
開　放
検出器
操作部
9
8
11
7
6
マイクロ
コントローラ
メモリ
独立
電源
302
1
入力
端子
R
G
B
2
認証・復号部
R
G
B
4
映　像
処理部
5
表示部
鍵データ
保持部
3
300
301
出力端子
201
映像信号出力装置
（セットトップボックス・
D－VHS）
200

【書類名】　　要約書

【要約】

【課題】　暗号化された映像信号の不正な取得や複製を、比較的簡単な方法でかつ効果的に防ぐことができる画像表示装置を提供する。

【解決手段】　認証・復号部２は、映像信号出力装置２００から入力された暗号化された映像信号を認証して復号する。開放検出器８は筐体１０の開放を検出する。メモリ７は、認証・復号部２における認証動作を有効とすることを示す第１のフラグと、認証動作を無効とすることを示す第２のフラグとのいずれかのフラグを記憶する。マイクロコントローラ６は、メモリ７のフラグに応じて認証・復号部２における認証動作を有効とするか無効とするかを制御する。開放検出器８によって筐体１０の開放が検出されたら、マイクロコントローラ６はメモリ７に第２のフラグを書き込む。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社